(19) Japanese Patent Office (JP)
(12) Patent Office Gazette (A)
(11) Laid-Open No. 154988/2001 (Heisei 13)
(P2001-154988A)
(43) Laid-open date: June 8, 2001
(21) Application No. 341288/1999 (Heisei 11)
(22) Application Date: November 30, 1999
(71) Applicant: 000006747
Ricoh Company, Ltd.
3-6, Nakamagome 1-chome, Ota-ku, Tokyo
(72) Inventors: Yoichi KANAI, Masuyoshi TANEUCHIDA, Tomio MIZUNO, Tatsuya FURUKAWA, Yoichi ISHIKAWA
c/o Ricoh Company, Ltd.
3-6, Nakamagome 1-chome, Ota-ku, Tokyo

[Title of the Invention] Electronic Information Disclosure Certifying Method and System, Recording Medium Where Electronic Information Disclosure Certifying Program is Stored

[Detailed Description of the Invention]

[0001]

[Technical Field Pertinent to the Invention]

The present invention relates to a method, a system and a program for certifying that electronic information has been disclosed on a network and a storage medium storing the program therein.

[0002]

[Prior Art]

A method and a system certifying that the electronic information was present on a specified date and at a specified time have been conventionally existent. Such methods and systems have been described in, for example, USP 5136647, US Re-examined Patent No. RE34954, USP 5136646, USP 5373561, USP 5781629 or the like. However, the art described in the above-mentioned US patents never certify that specified electronic information has been disclosed on a network such as internet.

[0003]

[Problem to be Solved by the Invention]

In recent years, the information technologies have been disclosed over internet or the like, such information technologies contain information equivalent to information technologies published in the forms of magazines or literatures or the like, the speediness of communications or the like are not to be compared with conventional periodicals. Therefore, many researchers have used internet or the like, aiming to earlier publish their own study results or the like. In addition, since the dispatch of information is more convenient and lower cost than those of the conventional periodicals, there may be high possibility that much more information is disclosed in the internet or the like. However, although one can certify that electronic information is presented in prior art, one can not certify that the electronic information is disclosed in the internet or the like. Namely, one could not judge whether or not electronic information was secret. In this case, if one can not certify that the information was disclosed in the internet or the like, there may be a fear that another person may obtain the patent with the same content as that of the disclosed technology. As stated above, the information technology disclosed in the internet or the like substantially has the same effect as that of the periodical, in Japan, the law is established not giving the patent to "an invention, which is available by the public through electronic communication circuits." However, since it is difficult to certify the fact that when the information technology disclosed in the internets or the like is disclosed or when they are altered, one can not deny aspects that the reliability of the information disclosed in the internet or the like as evidences is rather weaker than those of the conventional periodicals. Then, the present invention is intended to provided the method, the system and the computer program and the recording medium where the computer program is stored for certifying that electronic information has been disclosed under a predetermined condition on networks such as internet.

[0004]

[Means for Solving Problem]

In a specified computer connected to an internet of the first embodiment according to the present invention, the certifying method that a specified electronic information has been disclosed comprises a step for gaining access to the specified electronic information stored in the specified computer to copy the specified electronic information, a step for uniquely specifying the copied specified electronic information and attribute information containing information on the location of the specified electronic information on the network together with the date and time and obtaining an electronic certificate certifying them to store the electronic certificate and attribute information in a memory, and a step for providing the certification requester with the electronic certificate and attribute information stored in the memory, in response to a recording request. This

allows one to certify that one can gain access to an electronic information on a date and at a time of the certificate and at a designated location with an information (for example, URL (Uniform Resource Locator) on the location contained in the attribute information. The electronic information disclosure certifying method of the second embodiment according to the present invention comprises the first step for gaining access to the specified electronic information stored in the specified computer at a predetermined timing to copy the specified electronic information by every access and the second step for uniquely certifying that the copied specified electronic information and the attribute information containing the information on the location of the specified electronic information and access condition together with the date and time and obtaining the electronic certificate certifying them to store the electronic certificate and attribute information to the memory in response to a recording request. If this method is executed, one can certify that the electronic information has been disclosed on a network for a certain period of time as well. In addition, in the second embodiment according to the present invention, corresponding to the electronic certificate, a construction so as to contain the third step for storing the specified electronic information first copied in the memory may be also possible. Although the electronic information is kept at the recording requester, a centralized management together with the certificate or the like is implemented in the embodiment. Further, in the second embodiment according to the present invention, a construction so as to contain the fourth embodiment for providing the certification requester with the electronic certificate and attribute information stored in the memory may be also made. In addition, the fourth step as mentioned above may be also constructed so as to contain a step for providing the certification requester with the specified electronic information corresponding to the electronic certificate. In addition, the first step as mentioned above may be also constructed so as to contain a step for gaining access to the specified electronic information stored in the specified computer at a predetermined timing while changing an address at the origin of the access or a step for gaining access to the specified electronic information stored in the specified computer at a predetermined timing and at a predetermined frequency. What an unspecified computer can gain access to can be certified by changing the address at the origin of the access. In addition, gaining access at a predetermined frequency allows one to easily grasp the change of the electronic information or the like.

[0005]

In the second embodiment according to the present invention, a construction may be also made so as to further contain a step for causing a referential information making the specified electronic information accessible to be kept in a computer

connected to a network other than the specified computer connected to the network. This referential information allows the public in general to easily obtain the location of the electronic information, thereby enabling improvement of the availability of the electronic information by the public in general. It is preferable that this referential information is present and can be certified in any form. In the second embodiment according to the present invention, a construction so as to further contain a step for detecting whether or not a copy of the specified electronic information is changed and a step for storing the change in the memory if the change is detected may be also made. This allows the version shift of the electronic information to be recorded. Further in the embodiment according to the present invention, a construction so as to contain a step that the electronic information stored in the memory is disclosed in a computer other than the specified computer on a network so as to be able to retrieve it may be also possible. The availability of the electronic information by the public in general can be improved and any third party can use the electronic information with its certificate. In this regard, a construction so as to further contain a step that the abstract of the electronic information stored in the memory is disclosed in a computer other than the specified computer on a network so as to be able to retrieve it may be also possible. In the second embodiment according to the present invention, if the specified electronic information can be retrieved by an electronic information retrieval means provided on a network, a construction so as to further contain a step that the retrievability is stored in the memory may be also possible. What the specified electronic information can be retrieved by the electronic information retrieval means is to mean that its availability by the public in general is very high, and thus the admissibility of evidence of the specified electronic information is increased surprisingly. In addition, internet is most suitable for the network mentioned above, in this case, the electronic information may be a document that is described in mark-up languages such as HTML (Hyper Text Markup Language) and XML (eXtensibleMarkup Language), an information on the location of an electronic information on a network may be a uniform resource locator (URL), and an access condition may contain at least an IP address at the origin of the access.

[0006]

The system certifying that a specified electronic information has been disclosed in a specified computer connected to a network of the third embodiment according to the present invention has a means for gaining access to the specified electronic information stored in the specified computer to copy the specified electronic information, a means for uniquely specifying a copied specified electronic information and attribute information containing an information on the location of the specified electronic

information on a network together with the date and time and obtaining an electronic certificate certifying them to store the electronic certificate and attribute electronic information in the memory and a means for providing the electronic certificate and attribute electronic information stored in the memory in response to a recording request. In addition, the electronic information disclosure certifying system in the fourth embodiment according to the present invention has an access means for gaining access to the specified electronic information stored in the specified electronic information at a predetermined timing to copy the specified electronic information by every access, a means for uniquely specifying a copied specified electronic information and attribute information containing an information on the location of a specified electronic information on a network and an access condition together with the date and time and obtaining an electronic certificate certifying them to store the electronic certificate and attribute information in the memory and an issuing means for providing the certification requester with the electronic certificate and attribute information stored in the memory. In the fourth embodiment according to the present invention, a construction so as to further have a step for issuing an electronic certificate may be also possible. In addition, the modified example of the second embodiment described with regard to the second embodiment according to the present invention may be applied to the electronic information disclosure certifying system of the fourth embodiment. Further, the electronic information disclosure certifying systems of the first and second embodiments according to the present invention can be implemented as the program for executing the same with a computer, this program is stored, for example, in storage media or memories such as floppy disks, CD-ROM's, magneto-optical disks, semiconductor memories and hard disks.

[0007]

[Embodiments]

First, the overview of the services provided of the premise of the present inventions is described. For example, the requester A shall ask the home page provider B to perform the following items: (1) to record "the home page stored in his or her own WWW (World WideWeb) server connected to internet has been disclosed for a certain period of time", and (2) a link is attached to the home page in order for the public in general to know about the existent of the home page and the place of the existence. The service provider B who has received the request gains access to a home page at a designated URL from an IP address, which the requester A does not know at an arbitrary timing, which the requester A does not know, and copies the home page. Next, the service provider B generates attribute information containing the URL of the home page and the IP (Internet Protocol) address at the origin of the access, uniquely specifies a copy of the home page and

attribute information together with date and time and obtains an electronic certificate certifying them. And, the service provider B stores the copy of the home page and attribute information and an obtained electronic certificate corresponding thereto. The service provider B gains access to the home page at the designated URL again at an arbitrary timing, which the requester A does not know and copies the home page. In this case, the service provider B can additionally obtain a certification if the WWW server of the requester A does not implement an access restriction by gaining access thereto after changing the IP address at the origin of the access. Next, the service provider B generates an attribute information like the foregoing and uniquely specifies the copy of the home page and attribute information together with date and time and obtains an electronic certificate certifying them. And, the service provider B stores the copy of the home page and attribute information and obtained electronic certificate corresponding thereto. The service provider B repeats such processing for a certain period of time designated by the requester A. In addition, the service provider B publishes the linkage with the designated home page at the URL to the request in item (2) above on his or her home page of own WWW server connected to the internet, which may be accessible by the public in general. For example, there are cases where the linkage may be retrieved by every requester or every field of contents. In addition, the service provider has left the record that the linkage has been published on the WWW server together with that of the publishing period or the like. The requester A can ask the service provider B to provide the requester A with the recorded contents to the home page designated by the above item (1) when the former simultaneously requests the contents or when necessary. In response to the request, the service provider B provides the requester A with a copy of the saved home page, attribute information and electronic certificate. In this case, the service provider may write the afore-mentioned data on, for example, CD-R or the like and provide the same or may provide the data through the internet. Further, as a result of the above (2) item, there may be also a case where the service provider B provides the requester A with the records of what the linkage has been published on the designated home page and the period of time or the like as the certificates on the WWW server of the service provider B. The requester A can use the information provided from the service provider B as the certification that the home page has been disclosed on the internet for a certain period of time.

[0008]

The requester A can also ask the service provider B to provide the former with a record that the designated home page can be retrieved with (3) a search engine directed for the public in general on the internet besides items (1) and (2) mentioned above. This is evidence that the public in general was in a position to easily

know about the existence of the designated home page and the location of the existence. The service provider B performs retrieval with an appropriate key word or the like by an arbitrary search engine.

If the designated home can be retrieved, the service provider records a fact of what can be retrieved, the address and name of the search engine used, the key word used, the retrieving date or the like. There may be also a case where the service provider provides the requester with the records as the certificate in response to the record content provision request. Although the requester A asks to record the home page stored his or her on WWW server in item (1), (1) ' he or she can ask the service provider B to record the home page stored in another's WWW server. In this case, the service provider B implements a processing as described in the above item (1) similarly. However, there would be no guarantee that the home page of another's WWW server continues to exist for a certain period of time designated by the requester A, it may disappear, it may be altered. If the home page does not exist, the service provider B records the term that the home page is disclosed on internet is confirmed, there may also may be a case where the service provider B provides the requester A with the term in addition to information that he or she normally provides. If it is altered, if the foregoing process is implemented, the history of the alteration is left. In addition, the requester A may designate the URL of the home page stored in another's WWW server, or, for example, may also designate all URL's after implementing the designated key word retrieval with the designated search engine. In addition, the requester A can also ask (4) the service provider B to provide the requester A with the records of the version shifting of the home page stored in his or her own or another's WWW server. The service provider implements the processing as in item (1). However, the service provider B inspects whether or not the contents of the home page previously gained access and gained access this time are different from each other. If different, for example, the service provider records that this time is different from the previous time. In addition, the service provider B does not need to store a copy of the home page. For example, the requester A may merely store it. If the service provider B does not store the copy of the home page, what are stored by every access in the (1) and (1)' processings are only the attribute information and electronic certificate. In addition, in the case of item (4), if the contents of the home page previously gained access and gained access this time are different from each other, the change of the version can be stored by storing the difference thereof or storing the entire home page only if different or the like. In addition, the requester A can designate the recording period of time in the recording request, the number, the frequency or the like in the items (1) and (1)' . Further, the services in the items (2) to (4) can be options, particularly, the services in the items (2) and

(3) are unnecessary if the existence and location of the home page are available to the public in general in other media or the like.

[0009]

On the other hand, if the service provider B continues to provide the service, he or she retains many home pages with certificate that have been disclosed through the internet. Using this information, the service provider B (5) can implement home page provision services with electronic certificate. For example, the service provider B builds a data base that can performs a key word retrieval or the like through internets and provides a third party with retrieval services. And, in response to the recorded content provision request of a searcher S, the service provider provides the searcher S with the recorded contents through internet or in media such as CD-R. In addition, the service provider prepares the abstract of a home page with an electronic certificate, and there may be also a case where the service provider builds a database in a form that the abstract can perform the screening of the retrieval. The overview of the electronic information disclosure certifying system for providing the foregoing services is shown Fig. 1. The server A shown in 3, the server B shown in 5, the server C shown in 7, the server D shown in 9, the server E shown in 11 and many computers that are not illustrated are connected to the network 1. 1 that is the network, for example, is internet. The server A shown in 3 is a WWW server, which stores an electronic information, for example, the home page 31 whose URL is http://www.abcd.co.jp disclosed in the network 1. The server shown in 5 is the server controlled by the service provider contains the copy acquisition function 51, which gains access to an electronic information designated by a requester and obtains a copy thereof, for example, the attribute information generation function 53, which generates an information on the location of electronic information such as URL's and an attribute information containing an access condition, the certificate acquisition function 55, which uniquely certifies a copy of the electronic information and the attribute information together with the date and time and obtains an electronic certificate certifying them, the storage function 57, which stores necessary information, and the certificate provision function 59, which provides the electronic certificate or the like stored in response to the request of a requester. The memory 61 is connected to the server B shown in 5. The server C shown in 7 has the time stamp certificate issuing function 71, which uniquely certifies a specified electronic information together with the date and time and issues a certificate certifying them. The server C shown in 7 receives a certificate issuing request through the internet 1, the time stamp certificate issuing function 71 issues the electronic certificate, and returns the electronic certificate to the requester.

[0010]

The server D shown in 9 is the server for adding a function to the server B shown in 5, for example, publishes the link 91 to the home page designated by the requester as the WWW server. However, there may be also a case where the service provider creates a data base of the link 91 and can perform retrievals by each of contents and owner or the like of the home pages to be linked. Further, using the data of the memory 61 connected to the server B shown in 5, the data base 95 is created, there may be also a case where the server 95 shown in 9 holds the retrieval function 93, which can retrieve the data base 95 through a network. Further, it creates the abstracts of each of electronic information from the data of the memory 61, and there may be also a case where the retrieval function 93 can retrieve the data base 97 on the abstracts through the networks. The server E shown in 11 is the search engine directed for the public in general. The description of this search engine directed for the public in general is omitted since it remains unchanged with a conventional one. Next, the overview of the services (1) and (1) ' provided by the present invention are described as the workings of the system. The requester A, for example, designates a home page at a URL http://www.adcd.co.jp in the server A shown in 3 that should be recorded as an electronic information for a certain period of time, and asks the service provider B to provide the requester with the services (1) and (1)'. The service provider B performs the processings using the server B shown in 5. The copy acquisition function 51 in the server B shown in 5 gains access to the http://www.abcd.co.jp shown in the server A of Fig. 1 at an arbitrary timing, for example, through the route (A), and obtains a copy of the home page 31, for example, through the route (B). The copy thereof is stored in, for example, the main memory of the server B shown in 5. The copy acquisition function 51 stores IP addresses at the origins of the accesses in the memory by every access. The copy acquisition function 51 contains a function to determine access conditions, and, for example, determines whether or not to gain access using which timing and which IP address at the origin of the access. In addition, if the requester designates the frequency, accesses to be gained are scheduled to comply with the frequency. The attribute information generation function 53 generates attribute information containing an IP address at the origin of the access and a URL designated by the requester A. If the attribute information may contain the IP address of a proxy server and the dates and times on and at which accesses are gained, for example, if connected to the network 1 through the proxy server that is not illustrated by the server B shown in 5.

[0011]

The certificate acquisition function 55 obtains electronic certificates to the obtained copy of the home page 31 and the generated attribute information. For a

concrete processing, the details are described later. In the system in Fig. 1, for the certificate acquisition function 55, an electronic certificate issuing request that is issued, for example, though the route (C) of the network 1 is received by the time stamp certificate issuing function 71 of the server 7 shown in 7, the electronic certificate issued by the time stamp certificate function 71 is received, for example, through the route (D) of the network 1. The time stamp certificate function 71 is described in detail later. The storage function 57 stores a copy of the home page 31 obtained by the copy acquisition function 51, attribute information generated by the attribute information generation function 53 and an electronic certificate obtained by the certificate acquisition function 55 in the memory 61. However, it is arbitrary to store the copy of the home page 31 obtained by the copy acquisition function 51. For example, there may be a case where the requester A stores it by himself or herself. In addition, the storage function 57 may judge not to store the copy of the home page obtained this time if the content of previously copied home page 31 is exactly the same as that of the home page to which it gained access this time. In addition, the storage function 57 stores the data by every requester and every designated URL so as to allow the certificate provision function 59 to easily retrieve necessary data. The requester A asks the service provider to provide the requester A with the recorded contents at the same time as the recording is requested or at an arbitrary timing. In this case, the certificate provision function 59 reads out a copy of the home page 31, an attribute information and an electronic certificate that are the objectives by the request from the storage medium 61 in response thereto, stores the data in the storage media such as CD-R 63 in example of Fig. 1 and provides the requester A with the data. In addition, although a copy of the home page 31, attribute information and electronic certificate are stored by every access, the certificate provision function 59 may store all of them in a storage media such as CD-R and provide the requester with the data, if the copy of the home page 31 remains unchanged, it may provide the copy of the home page 31, all of the attribute information and all of the electronic certificates at a time when it gained access thereto for the first time. Further, it is also possible that in the certificate provision function 59, using the attribute information and electronic certificate, the access records containing the IP address at the origin of the access, the date and time of the electronic certificate are prepared, the access records, the home page 31 at a time when an access gained thereto for the first time, all of the attribute information, and all of the electronic certificates are provided as the certificates by the service provider B. In addition, if storage function 57 does not store the copy of the home page 31, the certificate provision function 59 does not provide the requester A with the copy of the home page 31 naturally as well.

[0012]

Next, the overview of the services provided by the present invention (2) is described based on the system shown in Fig. 1. (2) the requester A asks the service provider B to affix the link to the home page so as to allow the public in general to know about the existence of the home page and its location. In response to the request, the service provider B publishes the link 91 to the home page 31 stored in the server A shown in 3 in the server D shown in 9 connected to the network 1. If the number of requests is small, the service provider may merely publish the URL of the designated home page on the home page stored in the server D shown in 9. However, if the number of requests is large, there is also a case where the service provider B builds a data base on the link, and there may be a case where the service provider B arranges the home page so as to allow any third party to perform retrievals by the contents of the home page or kinds of businesses of the requesters. The service provider B stores the term that the link 91 to the home page 31 has been published on his or her own home page or the term that could be retrieved in the memory, when the service provider B is requested by the requester A or the like, the service provider B provides the record as a certificate. Next, the overview of the services (3) provided by the present invention is described based on the system shown in Fig. 1. (3) is the server E shown in 11 that is a search engine directed to the public in general on a network, and the requester ask the service provider B with the record that the home page can retrieved. The service provider B implements, for example, retrievals with appropriate key words or the like by a search engine in the server E shown in 11 through the server B shown in 5, if the designated home page 31 can be retrieved, the service provider B records the fact that can be retrieved and the name and address of the server E shown in 11, the key word used, the date of the retrieval or the like. When the request is made by the requester or the like later, the service provider provides this record as a certificate. Next, the overview of the services (4) provided by the present invention is described based on the system shown in Fig. 1. (4) is to ask the service provider B to provide the record of the version shifting of the home page 31. The service provider B implements the same processing as in (1) using the server B shown in 5. Namely, the service provider gains access to the home page 31 of the server A shown in 3 at a predetermined timing, and obtains a copy of the home page 31. Next, the service provider generates attribute information containing a URL and access conditions, and obtains certificates to the attribute information and the copy of the home page 31. And, the service provider stores at least the attribute information and electronic certificates in the storage 61. It is also possible that the provider stores the copy of the home page 31. Next, the service provider gains access to the home page 31 of the server A shown in 3 at a predetermined timing, implements a similar processing, and obtains certificates to the

attribute information copy of the home page 31. And, the service provider judges whether or not the content of the home page 31 to which the provider previously gained access, more correctly, of the home page 31 when the change is detected most recently and the contents of the home page 31 to which the provider gained access this time are different from each other. This judgment may be made by the copy acquisition function 51 or the storage function 57. If the contents thereof are different, the service provider records the difference in addition to at least the attribute information and electronic certificate in the memory. Depending on cases, the provider may record the difference between the contents of the home page 31 to which the service provider previously gained access and the service provider gained access this time, if different, the service provider may surely store the entire copy of the home page 31 in the memory. If the requester A or the like asks the service provider to provide the requester A with the data, the service provider B provides the requester A with at least attribute information and electronic certificate the record of whether or not the data is changed by the certificate provision function 59. The service provider may provide the entire home page by the difference or what is different.

[0013]

Next, the overview of the services (5) provided by the present invention is described based on the system shown in Fig. 1. (5) is a home page provision service with an electronic certificate. The service provider B provides the retrieval function 93 in the server D shown in 9 and creates the data base 95 using electronic certificates accumulated in the memory 61 and a copy of the home page 31 with the attribute information. And, the service provider allows a third party to retrieve the data base 95 from the retrieval function 93. If the third party finds the copy of the home page 31, which the third party wants to use, the third party provides the service provider B with a recorded content provision request through a network or the like. The service provider B stores the copy of the home page 31, attribute information and electronic certificate that are requested in, for example, CD-R 63 or the like using the certificate provision function 59, and provides the CD-R 63 or the like. The service provider may send the data as above-mentioned through the network 1. Further, it is also possible that the service provider B creates the abstract from the copy of the home page 31, builds the data base 97 of the abstract, and allows the third party to perform retrievals by the retrieval function 93. After the third party performs the screening on the data base of the abstract, the third party confirms the copy of the home pages 31 and can provide a necessary recorded content provision request of the electronic information. The processing flow of the major services (1) and (1)' according to the present invention is listed in Fig. 2. If the requester A provides the service provider B with an information on, for example, the recording objective

electronic information of the home page and, for example, the recording request where the recording conditions such as the recording period of time are designated (step S1), the copy acquisition 51 determines the access conditions so as to comply with the recording conditions (step 3), gains access to the URL at a predetermined timing from a predetermined IP address at the origin of the access to obtain a copy of the home page (step S5). And, the attribute information generation function 53 generates attribute information containing an IP address at the origin of the access as the URL of the home page and the access condition (step S7). Thereafter, the certificate acquisition function 55 specifies the attribute information and the obtained copy of the home page together with the date and time and obtains the certificate certifying them from the time stamp certificate issuing function 71 (step S9). In addition, it is also possible that the server B shown in 5 is constructed so as to contain the time stamp certificate issuing function 71, in this case, the certificate acquisition function 55 can be replaced with the time stamp certificate issuing function 71. And, the storage function 57 stores at least the attribute information and electronic certificate in the memory 61 (step S11). In addition, as stated above, whether or not to store a copy of the home page in the memory is arbitrary. And, this processing is repeated until the conditions of the recording completion are met (step S13). The condition of the recording completion is, for example, a case that the recording period of time designated by the requester A is completed or a case that the service provider reaches the number of recording designated by the requester A or the like.

[0014]

Fig. 3 shows an example of the processing flow in a case that the major services (1) and (1)' together with (4) according to the present invention are implemented. If the requester A asks the service provider B to provide the requester A with, for example, an information on the location of URL's of, for example, of the recording objective electronic information such as home pages and, for example, the designated recording conditions of the recording period of time or the like (step S21), the copy acquisition function 51 determines the access conditions so as to comply with the recording conditions (step S23), gains access to the URL at a predetermined timing from a predetermined IP address at the origin of the access to obtain a copy of the home page (step S25). And, the attribute generation function 53 generates the URL of the home page and the attribute information containing the IP address at the origin of the access as the access conditions (step S27). Thereafter, the certificate acquisition function 55 specifies the attribute information and a copy of the obtained home page together with the date and time and obtains the electronic certificate from the time stamp certificate issuing function 71 (step S29). In addition, it is also possible that the server B shown in 5 is constructed so as to contain the time stamp

certificate issuing function 71. Here, next, the storage function 57 inspects whether or not the contents of the home page the service provider previously accessed and the home page the service provider gained access this time has been changed (step S31). For the inspection, the copy of the home page is read out when the latest change stored in the memory 61 is detected, which is compared with the copy of the home page the service provider gained access this time. If the change is detected, the home page, the electronic certificate and attribute information that are associated with each other and are stored in the memory (step 33). On the other hand, if the change is not detected, the certificate and attribute information are stored in the memory (step 35). Such a processing is repeated until the condition of the recording completion is met (step 37). If the processing flow as shown in Fig. 3 is implemented, for example, the information shown in Fig. 4 is stored, the home page shifting of the designated URL can be certified. In fig. 4, since all has been changed at the time of the first access, the copy of the home page, the electronic certificate and attribute information are stored in the memory. At the time of the second access, the of the home page stored at the time of the first access and the copy of the home page the service provider gained access this time are compared, it is judged that nothing has been changed, only the electronic certificate and attribute information are stored. At the time of the third access, the copy of the home page stored at the time of the first access and the copy of the home page the provider gained access this time are compared, it is judged that nothing has been changed, only the electronic certificate and attribute information are stored. At the time of the fourth access, the copy of the home page stored at the time of the first access and the copy of the home page accessed this time are compared, it is judged that the change has been detected, the copy of the home page accessed at the time of the fourth access, electronic certificate and attribute information are stored. The following processings are implemented if the change has been detected or nothing has been found. The objective of the comparison is the copy of the home page that is stored since the latest changed has been detected.

[0015]

Next, Fig. 5 shows the processing flow that is executed in response to a recorded content provision request by the requester A. Since the electronic information that is the objective is contained in the recorded content provision request (step S41), the certificate provision function 59 first specifies the electronic information that is the objective (step S43). And, the certificate provision function 59 reads out a copy of the objective electronic information, electronic certificate and attribute information from the memory 61 (step S45). In addition, if the recording of only one time is requested, or if the objective electronic information disappears accordingly by only one access, although the data that is

read out is only one set, since it is recorded usually a plurality of times, a plurality of sets of a copy of the electronic information, attribute information and electronic certificate are read out. And, the certificate provision function 59 additionally calculates the disclosure term (step S47). Since the record of date and time is contained in the electronic certificate, if the electronic certificate obtained at the time of the first access and the electronic certificate accessed lastly are referred to, it can be known at least from when to when the home page has been disclosed. This information is determined to be the disclosure term. However, this processing is arbitrary. Lastly, the certificate provision function 59 stores the copy of the objective electronic information, electronic certificate and attribute information in, for example, media such as CD-R's to provide the same.

[0016]

Here, the electronic certificate is briefly described using Fig. 6. In the present invention, if the electronic information together with date and time are uniquely specified and the electronic certificate certifying them is issued, the electronic certificate may be issued in any system. Therefore, the following description is one example, the electronic certificate may be issued in other systems. If the electronic information 101 is assumed to be the objective of an electronic certificate, first, the hash value 103 is calculated to the electronic information 101. Hash function may be any functions if it is one directional function. For example, the certificate acquisition function 55 performs up to the calculation of the hash value. And, the issuing request of the certificate containing this hash value 103 is sent to the time stamp certificate issuing function 71. The time stamp certificate issuing function 71 processes the same together with other hash values sent similarly. For example, as in Fig. 6, the processing that another hash value is generated from the two hash values is repeated, and the one hash value 106 is finally generated from all the hash values sent. SHV 107 is generated at the time T using this hash value 106 and SHV (Super Hash Value) 105 at the time, T-1 (T is an integer). SHV 107 thus generated at the time T and the hash value 103 and the time information at the time T, the document ID constitute the electronic certificate 109. This electronic certificate 109 is sent to the sender of the hash value 103, the electronic information 101 and the electronic certificate 109 are to be a pair, the electronic information 101 together with the date and time can be uniquely specified and certified. In addition, if the home page that is the electronic information is made in accordance to the electronic information in Fig. 6, a HTML document is equivalent to the electronic information. Therefore, as shown in Fig. 7, the hash value is calculated from the attribute information 111 containing the HTML document 110, the URL and the IP address at the origin of the access or the like, the electronic certificate is prepared from the hash value. If the contents of the home page is

only sentences, it is sufficient. However, an image file such as GIF file is often embedded in the home page. In this case, since the contents of the image files of GIF files or the like are included in the information disclosed on the internet, the hash value is calculated from this image file, HTML document and attribute information. Further, not only static images, but also dynamic images, sounds, files of performances requiring the plug-in of a browser or the like, or Java (the trademark of Sun Microsystems, Inc.) manufactured-applet are embedded in HTML documents. If these objects are embedded, these are copied at the time of an access to the designated URL, and they are used for the hash value calculation. The hash value may be calculated by each file or one hash value for all files may be calculated.

[0017]

Thus, a fact that the electronic information has been disclosed can be certified by the overview of the services (1) and (1)' according to the present invention. A fact that the existence and location of the electronic information are known to the public in general can be certified by (2) and (3). In addition, the version shifting of the electronic information can be grasped by (4). Further, the service provider can more effectively use the electronic information with electronic certificate by (5). The requester can promote the utilization of the electronic information by the public in general, and a third party can obtain the electronic information with admissibility of evidence that is not held by himself or herself. With such systems, for example, in the fields of patents, they can use the attribute information and electronic information with an electronic certificate for evidences at filing an opposition to a patent or filing the invalidity of a patent in patent-related disputes. In addition, a home page or the like can be used like a disclosed technical report. In addition, it can also be also used as evidence for the application of exception of loss of the novelty. The contents mentioned above are only some examples, and various forms are possible. For example, the five functions contained in the server B shown in 5 are contained in one server in Fig.1. However, it is also possible that they are dispersed in a plurality of servers. Similarly, in the server D shown in 9, the requested link to the home page is published, and the retrieval function is also provided. However, it is also possible that these can be executed in individual servers. The search engine directed to the public in general connected to the network 1 is not limited to one search engine. In addition, not only a ftp can be also used. It is also possible that the function of the server C shown in 7 can be included in that of the server B shown in 5. The principal that executes the service by the server C shown in 7 and the principal that executes the service by the server B shown in 5 may be separate or the same. The network 1 is not limited to internet, but can be expanded up to a network that allows a user to gain access to another's non-exclusive

networks and a network where a user wanting to use a network is non-exclusively treated. Although media for providing recorded contents are determined to be CD-R 63, this is also one example, but may be other media, for example, CD-ROM or DVD. In addition, how to divide the functional blocks shown in Fig. 1 is also one example, it is possible that one functional block can be also divided into a plurality of functional blocks, and a plurality of functional blocks can be also integrated into one functional block. It is also possible that the device shown in Fig. 1 is constructed or a part or the whole thereof are executed by dedicated circuits or the like.

[0018]

[Effect of the Invention]

The method, system, and computer program and recording media where the computer program is stored can be provided to certify that a specified electronic information has been disclosed under a predetermined condition on networks such as internets

[Brief Description of Drawings]

[Fig. 1] A block diagram showing the overview of the system in the present invention.

[Fig. 2] A flowchart showing one example of the processings executed in response to an electronic information recording request.

[Fig. 3] A flowchart showing one example of the processings executed in response to an electronic information recording request.

[Fig. 4] A mimetic diagram showing one example of kinds of information stored by every access to electronic information.

[Fig. 5] A flowchart showing one example of the processings executed in response to a recorded content provision request.

[Fig. 6] A mimetic diagram showing one example of the issuance processings of an electronic certificate specifying the electronic information together with date and time and certifying them.

[Fig. 7] A mimetic diagram for describing the generation of a hash value executed in the issuance processing in Fig. 6.

[Description of Reference Numerals]

1: Network

3: Server A

5: Server B

7: Server C

9: Server D

11: Server E
31: Home page
51: Copy acquisition function
53: Attribute information generation function
55: Certificate acquisition function
* 57: Storage function
59: Certificate provision function
61: Memory
63: CD-R
71: Time stamp certificate issuing function
91: Link
93: Retrieval function
97: Abstract data base
101: Electronic information
103: Hash value
105: SHV at time T-1
106: Hash value
107: SVH at time T
109: Electronic certificate
110: HTML document
111: Attribute information
112: Image file

[Claims]

1. An electronic information disclosure certifying method that certifies that specified information has been disclosed in a specified computer connected to a network characterized by comprising:

a step for making an access to said specified electronic information stored in said computer in response to a recording request and copying said specified electronic information;

a step for uniquely specifying a copy of said specified electronic information and the attribute information containing the information on the location of said specified electronic information on said network together with the data and time and obtaining an electronic certificate certifying them to store the electronic certificate and said attribute information in a memory; and

a step for providing the certification requester with said electronic certificate and said attribute information stored in said memory.

2. The electronic information disclosure certifying method that certifies that specified information has been disclosed in a specified computer connected to a network characterized by comprising:

a first step for making an access to said specified electronic information stored in said computer at a predetermined timing in response to a recording request and copying said specified electronic information by each access; and

a second step for obtaining an electronic certificate uniquely specifying and certifying said copied specified electronic information and the attribute information containing the information on the location of said specified electronic information and the access condition on said network together with the date and time to store the certificate and said attribute information in the memory.

3. The electronic information disclosure certifying method according to claim 2, wherein a third step for storing said first copied electronic information to the memory in response to said electronic certificate is further contained.

4. The electronic information disclosure certifying method according to claim 2, wherein a fourth step for providing the certification requester with said electronic certificate and said attribute information stored in said memory is further contained.

5. The electronic information disclosure certifying method according to claim 4,

wherein a step that said fourth step provides the certification requester with said specified electronic information corresponding to said electronic certificate is contained.

6. The electronic information disclosure certifying method according to claim 2, wherein a step that said fourth step gains access to said specified electronic information stored in said specified computer at a predetermined timing while changing an address at the origin of the access is contained.

7. The electronic information disclosure certifying method according to claim 2, wherein a step that said first step gains access to said specified electronic information stored in said specified computer at a predetermined timing and a predetermined frequency. is contained.

8. The electronic information disclosure certifying method according to claim 2, wherein a step that causes a computer connected to other than said network for said specified computer to hold referential information for allowing said specified electronic information to gain access is further contained.

9. The electronic information disclosure certifying method according to claim 2, wherein a step for detecting whether or not said copied specified electronic information is changed and a step for storing the change in the memory if the change is detected are further contained.

10. The electronic information disclosure certifying method according to claim 3, wherein a step that said specified electronic information stored in said memory is disclosed in a computer other than said specified computer on said network so as to be retrieved is further contained.

11. The electronic information disclosure certifying method according to claim 3, wherein a step that the abstract of said specified electronic information stored in said memory is disclosed in a computer other than said specified computer in said network so as to be retrieved is further contained.

12. The electronic information disclosure certifying method according to claim 2, wherein a step that causes the memory to store the retrievability if said specified electronic information can be retrieved by electronic information retrieval means provided on said

specified network is further contained.

13. The electronic information disclosure certifying method according to claim 2, wherein if said network is internet, said electronic information is a document that is described in mark-up language, information on the location of said electronic information on said network is a uniform resource locator, namely, said access conditions contain at least an IP address at the origin of the access.

14. An electronic information disclosure certifying system that is a system certifies that specified electronic information has been disclosed in a specified computer connected to a network, wherein the system has:

a means for gaining access to said specified electronic information stored in said specified computer in response to a recording request to copy said specified electronic information;

a means for uniquely specifying a copy of said specified electronic information and an attribute information containing an information on the location of said specified electronic information on said network together with the date and time and obtaining an electronic certificate certifying them to store the electronic certificate and said attribute electronic information in a memory; and

a means for providing said electronic certificate and said attribute electronic information stored in said memory.

15. An electronic information disclosure certifying system that is a system certifying that specified electronic information has been disclosed in a specified computer connected to a network, wherein the system has:

an access means for gaining access to said specified electronic information stored in said specified computer at a predetermined timing and copying said specified electronic information by every access in response to a recording request;

a storing means for uniquely specifying a copy of said specified electronic information and an attribute information containing information on the location of said specified electronic information on said network and an access condition together with the data and time and obtaining an electronic certificate certifying them to store the electronic certificate and attribute information in a memory; and

an issuing means for providing the certification requester with said electronic certificate and said attribute information stored in said memory.

16. The electronic information disclosure certifying system according to claim 15, wherein the system further has a means for issuing said electronic certificate.

17. The electronic information disclosure certifying system according to claim 15, wherein said memory stores a copy of said electronic certificate first obtained in response to said electronic certificate.

18. The electronic information disclosure certifying system according to claim 17, wherein said providing means provides said certification requester with said specified electronic information stored in said memory corresponding to said electronic certificate.

19. The electronic information disclosure certifying system according to claim 15, wherein said access means gains access to said specified electronic information stored in said specified computer at a predetermined timing while changing an address at the origin of the access.

20. The electronic information disclosure certifying system according to claim 15, wherein said access means gains access to said specified electronic information stored in said specified computer at a predetermined timing and a predetermined frequency.

21. The electronic information disclosure certifying system according to claim 15, wherein a computer other than said specified computer that stores referential information that causes said specified electronic information to be accessible and is connected to said network is further contained.

22. The electronic information disclosure certifying system according to claim 15, wherein the system further has a means for detecting whether or not said copied specified electronic information is changed and storing the change if the change is detected to said memory.

23. The electronic information disclosure certifying system according to claim 15, wherein the system further has a computer other than said specified computer connected to said network that can store and retrieve said specified electronic information.

24. The electronic information disclosure certifying system according to claim 15, wherein the system further has a computer other than said specified computer connected

to said network that can store and retrieve the abstract of said specified electronic information.

25. The electronic information disclosure certifying system according to claim 15, wherein said memory can store the retrievability if it can retrieve said specified electronic information by the electronic information retrieval means provided on said network.

26. The electronic information disclosure certifying system according to claim 15, wherein if said network is internet, said electronic information is a document that is described in mark-up language, information on the location of said electronic information on said network is a uniform resource locator, namely, said access conditions contain at least an IP address at the origin of the access.

27. A storing medium that stores a program to certify that specified electronic information has been disclosed in a specified computer connected to a network, wherein said program contains:

a step for causing a computer other than said specified computer to gain access to said specified electronic information stored in said specified computer in response to a recording request to copy said specified electronic information;

a step for uniquely specifying said copied specified electronic information and an attribute information containing information on the location of said specified electronic information on said network together with date and time and obtaining an electronic certificate certifying them to store the electronic certificate and said attribute information in a memory; and

a step for providing the certification requester with said electronic certificate and said attribute information stored in said memory.

28. A recording medium that stores a program to certify that specified electronic information has been disclosed in a specified computer connected to a network, wherein said program contains:

a first step for causing a computer other than said specified computer to gain access to said specified electronic information stored in said specified computer at a predetermined timing in response to a recording request and copying said specified electronic information by every access; and

a second step for uniquely specifying said copied specified electronic information and an attribute information containing an information on the location of said specified

electronic information and an access condition together with the date and time and obtaining an electronic certificate certifying them to store the electronic certificate and said attribute information in a memory.

[Abstract]

[Problem] To certify that electronic information is disclosed under a predetermined condition on networks such as internet.

[Solving means] An service provider B gains access to the home page of the URL designated by an a requester A, copies the home page, creates an attribute information containing the URL and an IP address at the origin of the access or the like, uniquely specifies the copied home page and the attribute information together with the date and time, and obtains an electronic certificate certifying them, and stores them corresponding to the copy of the home page and attribute information. The service provider B repeats this for a designated period of time. The requester A asks the service provider B to provide the requester A with the recorded contents of the designated home page simultaneously at the request thereof, or when necessary. At the request of the requester A, the service provider B provides the requester A with copies of the stored home page, attribute information and electronic certificate. In addition, the service provider B provides the requester A with a record that the link of the WWW server of the service provider B with the designated home page is listed on his or her server and the period of time or the like as the certificate.

FIG. 1

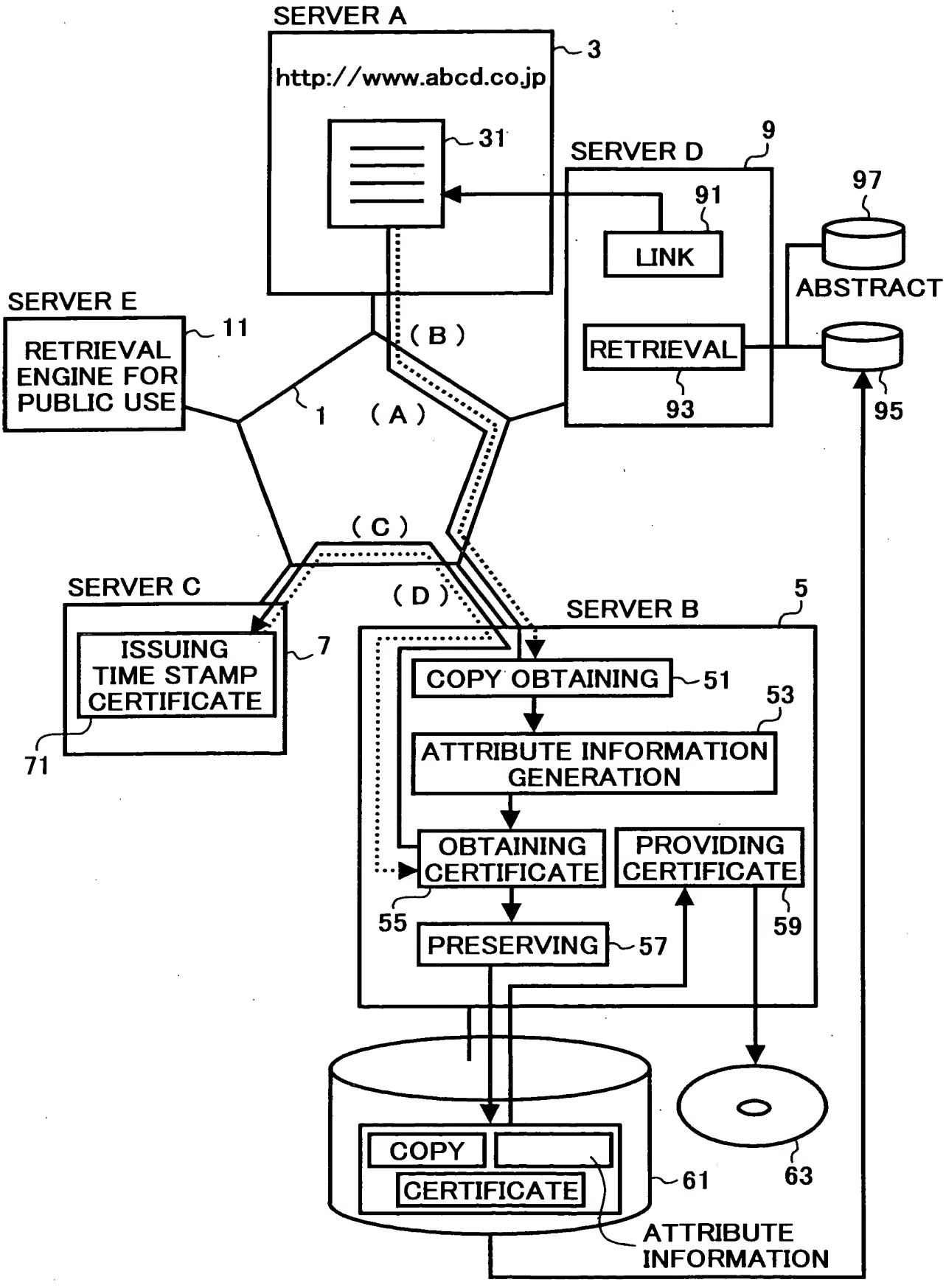

SERVER A
http://www.abcd.co.jp
3
31
SERVER D
9
91
LINK
97
ABSTRACT
SERVER E
RETRIEVAL ENGINE FOR PUBLIC USE
11
(B)
RETRIEVAL
93
95
1
(A)
(C)
SERVER C
(D)
SERVER B
5
ISSUING TIME STAMP CERTIFICATE
7
71
COPY OBTAINING
51
53
ATTRIBUTE INFORMATION GENERATION
OBTAINING CERTIFICATE
PROVIDING CERTIFICATE
55
59
PRESERVING
57
COPY
CERTIFICATE
61
63
ATTRIBUTE INFORMATION

FIG. 2

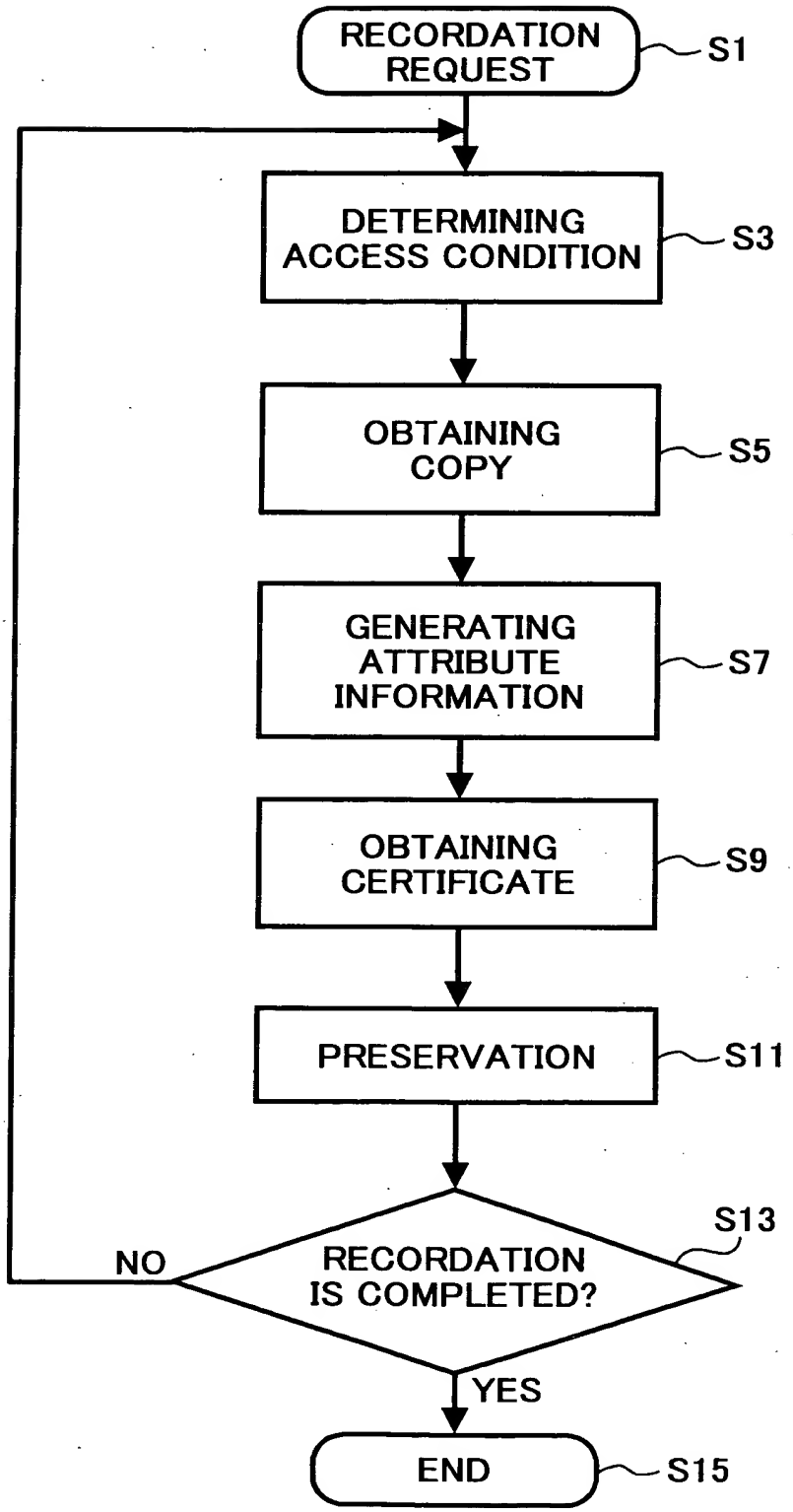

RECORDATION REQUEST
S1
DETERMINING ACCESS CONDITION
S3
OBTAINING COPY
S5
GENERATING ATTRIBUTE INFORMATION
S7
OBTAINING CERTIFICATE
S9
PRESERVATION
S11
RECORDATION IS COMPLETED?
S13
NO
YES
END
S15

FIG. 3

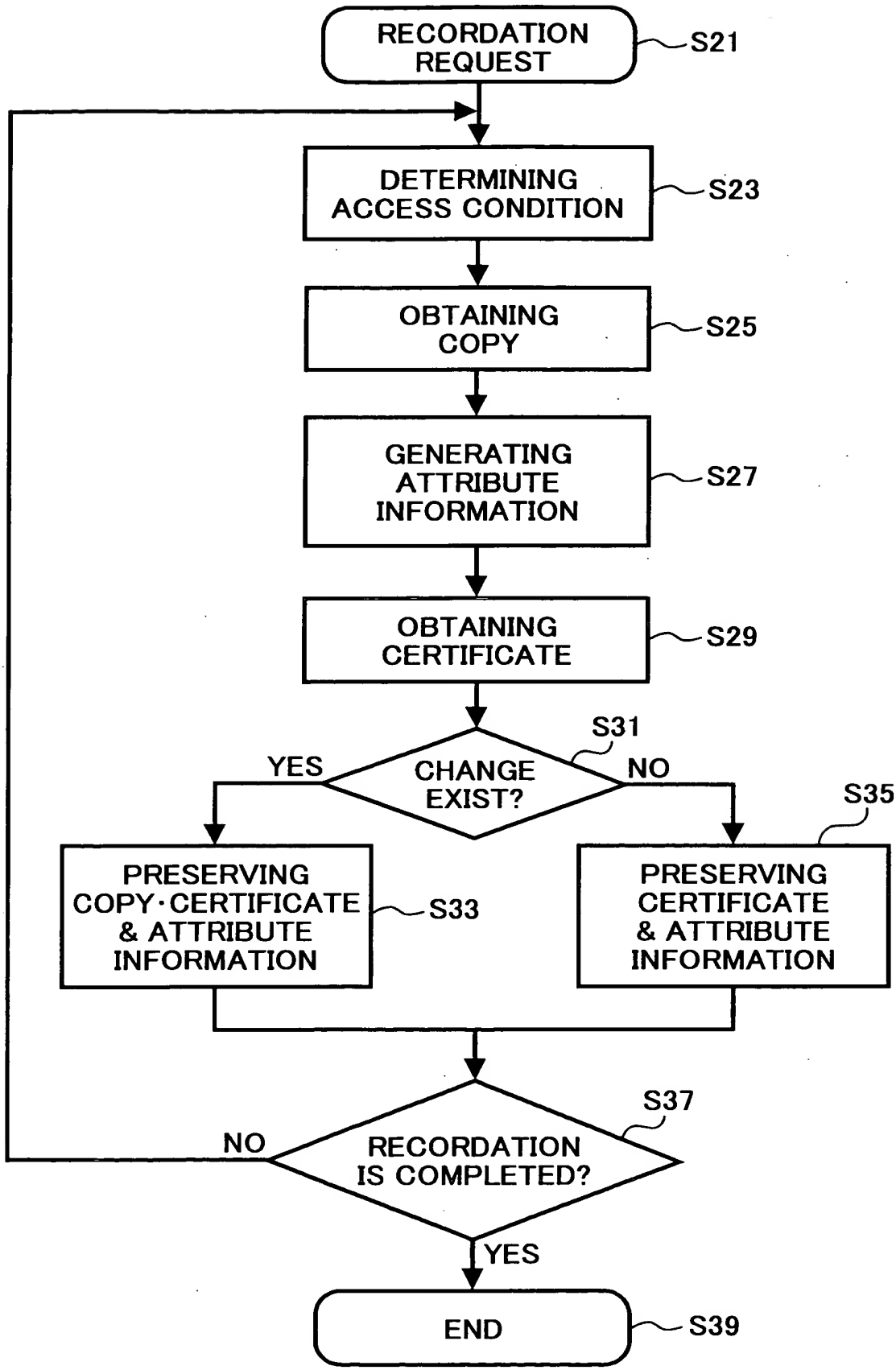

RECORDATION REQUEST
S21
DETERMINING ACCESS CONDITION
S23
OBTAINING COPY
S25
GENERATING ATTRIBUTE INFORMATION
S27
OBTAINING CERTIFICATE
S29
S31
CHANGE EXIST?
YES
NO
PRESERVING COPY·CERTIFICATE & ATTRIBUTE INFORMATION
S33
S35
PRESERVING CERTIFICATE & ATTRIBUTE INFORMATION
S37
RECORDATION IS COMPLETED?
NO
YES
END
S39

FIG. 4

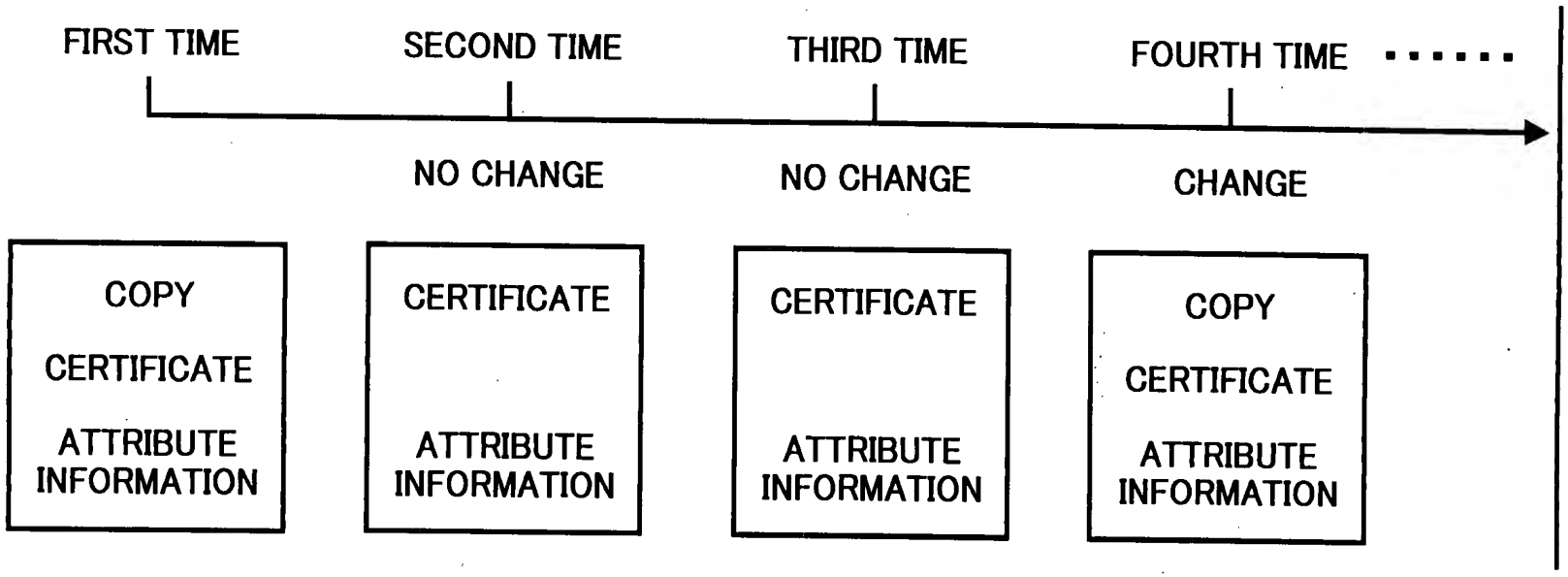

FIRST TIME
SECOND TIME
THIRD TIME
FOURTH TIME
NO CHANGE
NO CHANGE
CHANGE
COPY
CERTIFICATE
ATTRIBUTE INFORMATION
CERTIFICATE
ATTRIBUTE INFORMATION
CERTIFICATE
ATTRIBUTE INFORMATION
COPY
CERTIFICATE
ATTRIBUTE INFORMATION

FIG. 5

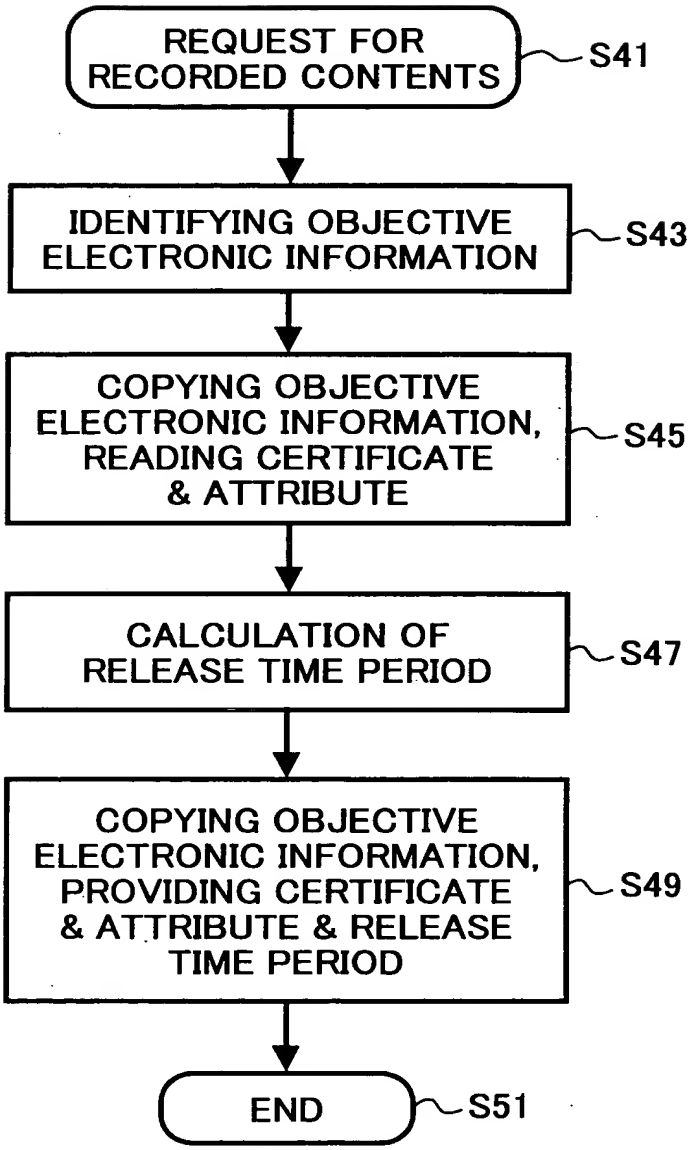

REQUEST FOR RECORDED CONTENTS
S41
IDENTIFYING OBJECTIVE ELECTRONIC INFORMATION
S43
COPYING OBJECTIVE ELECTRONIC INFORMATION, READING CERTIFICATE & ATTRIBUTE
S45
CALCULATION OF RELEASE TIME PERIOD
S47
COPYING OBJECTIVE ELECTRONIC INFORMATION, PROVIDING CERTIFICATE & ATTRIBUTE & RELEASE TIME PERIOD
S49
END
S51

FIG. 6

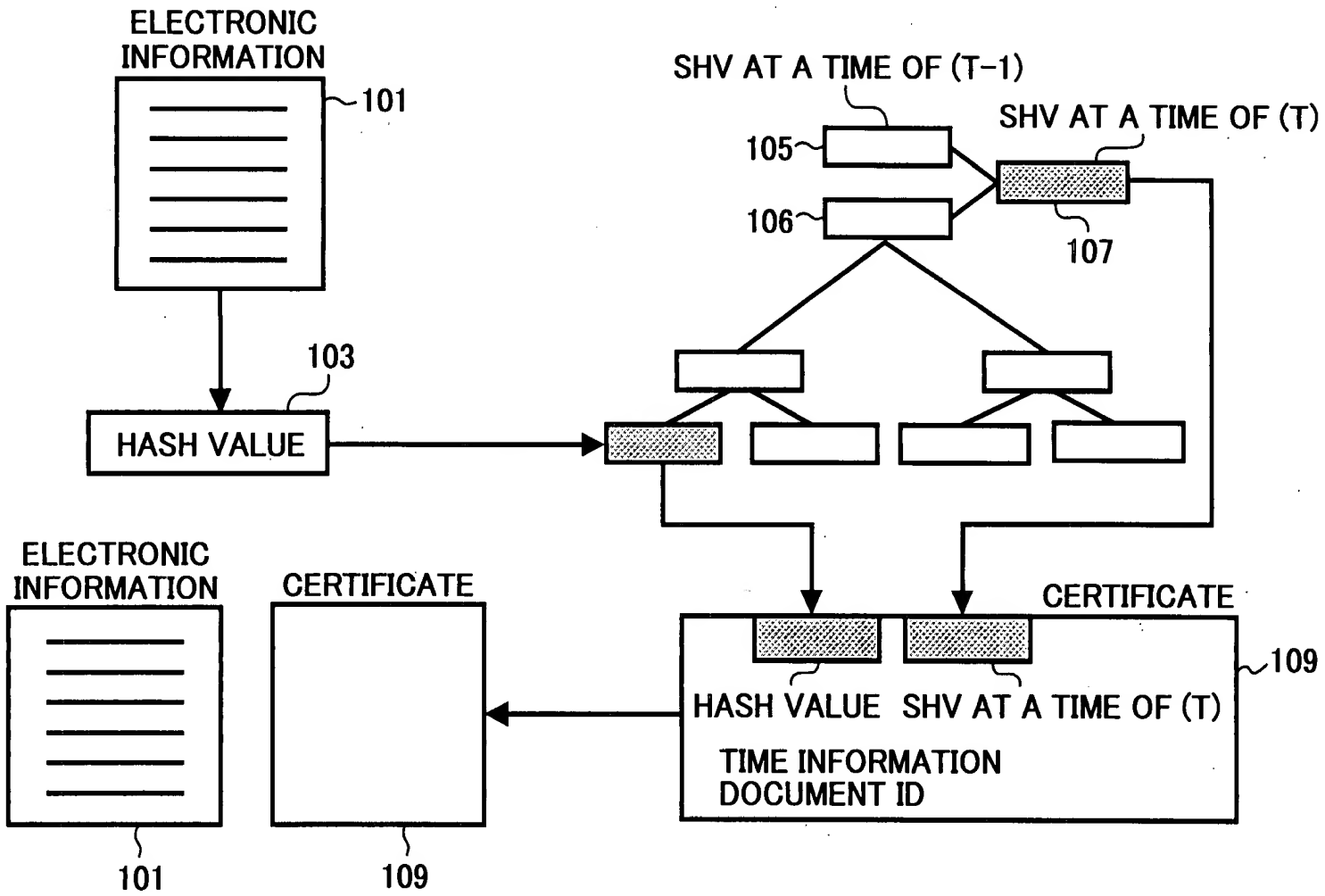
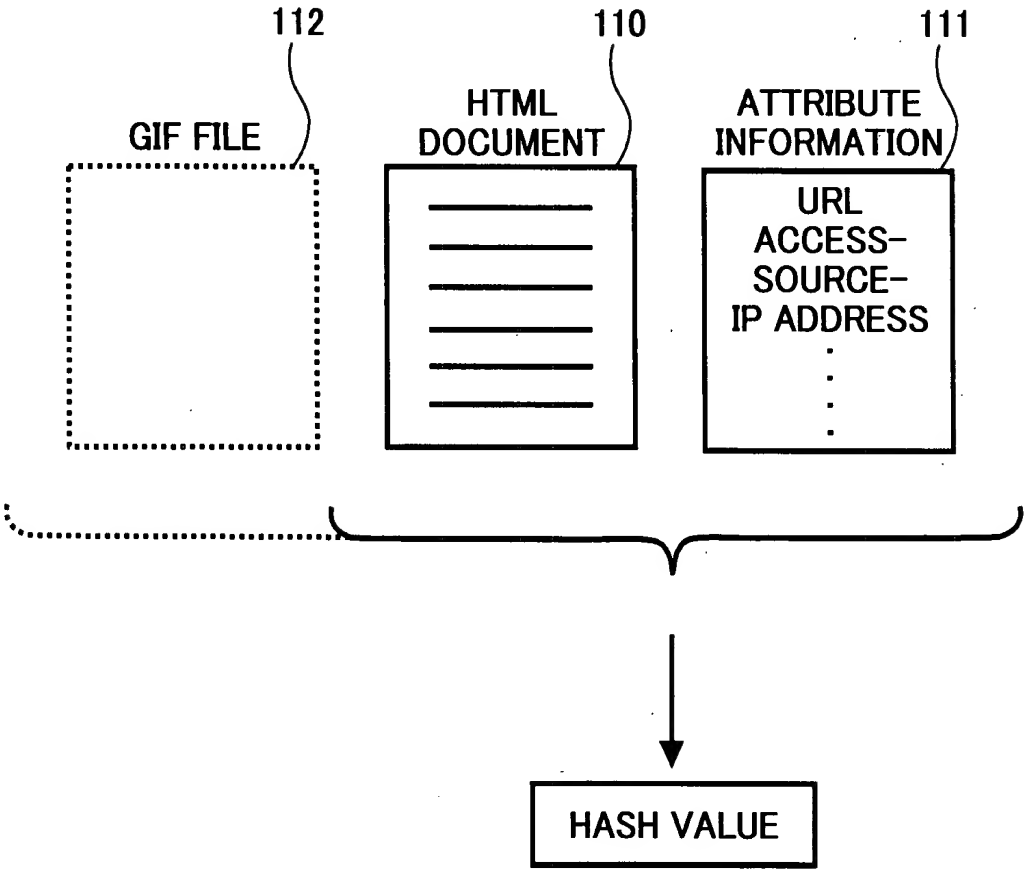

ELECTRONIC INFORMATION
101
SHV AT A TIME OF (T-1)
SHV AT A TIME OF (T)
105
106
107
103
HASH VALUE
ELECTRONIC INFORMATION
CERTIFICATE
CERTIFICATE
109
HASH VALUE
SHV AT A TIME OF (T)
TIME INFORMATION
DOCUMENT ID
101
109

FIG. 7


112
110
111
GIF FILE
HTML DOCUMENT
ATTRIBUTE INFORMATION
URL
ACCESS-SOURCE-IP ADDRESS
HASH VALUE